BESSEGGEN PASSWORD POLICY

Doc: Version: 1.4

Document Classification: Internal

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

Document Control

Document Name	Besseggen Password Policy
Abstract	This document describes the password related policies at Besseggen Infotech LLP.
Security Classification	Internal
Location	SECTOR-94, NOIDA, GAUTAM BUDH NAGAR-201301

Authorization		
Document Owner	Reviewed by	Authorized by
IT Team	Head – IT	Head – IT

Amendment Log				
Version	**Modification Date**	**Section**	**A/M/D**	**Brief description of change**
1.1	01 Apr 2022	ALL	A	Final
1.2	10 Apr 2022	3	M	Reviewed
1.3	13 May 2024	ALL		Reviewed
1.4	30 May 2025	ALL		Reviewed

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

Distribution list
Chief Information Security Officer (CISO)
Auditors (Internal & External)
All users,committee at Besseggen Infotech LLP.

TABLE OF CONTENTS

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

1. Purpose

The purpose of this policy is to define the standard for creating strong passwords for all users. Password security, password changes, and other password rules help protect the Besseggen Infotech technology resources from harmful acts.

2. Scope

The scope of this policy includes all users. Users are defined as anyone with authorised access to the Besseggen Infotech technology resources, including permanent and temporary employees or third party personnel such as temporaries, contractors, consultants, and other parties with valid access accounts.

3. Policy Statement

Passwords are an important aspect of computer security and are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Besseggen Infotech internal network. Users of Besseggen Infotech technology resources are therefore responsible for taking appropriate steps in selecting and securing their passwords.

DEFINITIONS:
Technology Resources: All computing, networking, and software applications that can be accessed by authorised users.

4. Responsibility for Policy

The HEAD – IT is responsible for development, maintenance, implementation, operation and escalation of enforcement of these policies and standards.

5. Procedures

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

Password Use Policy:

User passwords are sensitive, confidential information and must not be shared with others. Passwords are the first line of protection against threats to network security, whether threats originate internally or externally.

- Minimum Password Length & complexity
  - Wherever the system or application can accommodate, passwords must be a minimum of eight characters in length.
  - A combination of alphabets ,numbers and special characters should be used

- Minimum Password Age
  - Password age refers to the time during which a password must be used before a new password can be selected. New password shall not be same as of the previous 6 passwords
- Password Expiration and History Management Policy
  - The standard expiration period is 14 days. No user account is set to non-expire.
  - Passwords must not be repeated within 6 generations.

- Password Lockout Policy
  - Users are locked out of their account after three failed logon attempts. Failed logon attempts are the result of attempting to logon using either a faulty logon ID (user name) or password.
  - The lockout period remains in force until removed by system administrator.

- Temporary Passwords
  - First-time Besseggen Infotech computer users (or those requiring a password reset) are given a temporary password that must be changed immediately after the first login.

For All Trading Applications:

User passwords are sensitive, confidential trading information and must not

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

be shared with others. Passwords are the first line of protection against threats to network security, whether threats originate internally or externally.

- Minimum Password Length & complexity
  - Wherever the application can accommodate, passwords must be a minimum of six and maximum of twelve characters in length.
  - A combination of alphabets & numbers. Preferably with one special characters
  - Login id of the user and password should be different

- Minimum Password Age
  - Password age refers to the time during which a password must be used before a new password can be selected. New password shall not be same as of the previous 3 passwords

- Password Expiration and History Management Policy
  - The exchange's standard expiration period is 14 days.
  - For IBT applications, the standard expiration period is 60 days.
  - No user account is set to non-expire.
  - Passwords must not be repeated within 3 generations.

- Password Lockout Policy
  - Users are locked out of their account after three failed logon attempts. Failed logon attempts are the result of attempting to logon using either a faulty logon ID (user name) or password.

- Temporary Passwords
  - First-time trading application users (or those requiring a password reset) are given a temporary password that must be changed immediately after the first login.

Secure Password Guidelines :

The following guidelines are valid throughout Besseggen Infotech to protect information and enhance the security of the network:

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

- If accounts or passwords have been compromised, report the incident to IT Support and change all passwords immediately.
- If an administrator requires that you login to a machine or service, use precautions so that password(s) are not witnessed.
- Anyone demanding a password must be reported to IT Support.
- Users shall not choose passwords, which can be easily guessed such as the user's name, car registration number, telephone number, birth date etc.
- All vendor-supplied default passwords (or other alternative access mechanisms) must be changed before any computer or communications system is used for any business activity beyond initial evaluation in a test environment. These standards apply to passwords associated with end-user user IDs, as well as passwords associated with systems administrator and other privileged user IDs.
- Users shall not share their password with anyone, including their reporting supervisors or colleagues.
- Passwords should not be written down or left in a place where unauthorized persons might discover them.
- Passwords shall not be stored unencrypted in system resources.
- Appropriate procedures shall be put in place for storing and management of administrative passwords for critical information systems.

6. Enforcement

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or legal action as appropriate, or both. No provision of this policy will alter the at-will nature of the employment relationship at Besseggen Infotech LLP.

7. References

- NA

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3
FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301
LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)